WHAT IS CLAIMED IS:

1. A method for protecting publicly accessible network computer services from undesirable network traffic in real-time, the method comprising:

receiving network traffic destined for the services;

analyzing the network traffic to identify an undesirable user of the services; and

limiting access of the undesirable user to the services to protect the services.

2. The method as claimed in claim 1 wherein the undesirable network traffic includes denial of service attacks.

3. The method as claimed in claim 1 wherein the network is the Internet.

4. The method as claimed in claim 1 further comprising generating one or more user profiles from the network traffic wherein the step of analyzing includes the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user.

5. The method as claimed in claim 4 wherein the step of generating the one or more user profiles includes the step of generating request statistics for the user from the network traffic.

6. The method as claimed in claim 5 wherein the request statistics include connection statistics and service request distributions.

7. The method as claimed in claim 6 wherein the network is the Internet and wherein the step of generating request statistics includes the steps of collecting and correlating Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions.

8. The method as claimed in claim 7 wherein the step of correlating includes the step of identifying a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines.

9. A system for protecting publicly accessible network computer services from undesirable network traffic in real-time, the system comprising:

an interface for receiving network traffic destined for the services;

a analysis engine for analyzing the network traffic to identify an undesirable user of the services; and

a forwarding engine in communication with the analysis engine for limiting access of the undesirable user to the services to protect the services.

10. The system as claimed in claim 9 wherein the undesirable network traffic includes denial of service attacks.

11. The system as claimed in claim 9 wherein the network is the Internet.

12. The system as claimed in claim 9 wherein the forwarding engine generates one or more user profiles from the network traffic and wherein the analysis engine compares the one or more user profiles with a predetermined profile to determine the undesirable user.

13. The system as claimed in claim 12 wherein the forwarding engine generates the user profile by generating request statistics for the user from the network traffic.

14. The system as claimed in claim 13 wherein the request statistics include connection statistics and service request distributions.

15. The system as claimed in claim 14 wherein the network is the Internet and wherein the forwarding engine collects and correlates Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions.

16. The system as claimed in claim 15 wherein the forwarding engine identifies a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines.